

# A nearly tight upper bound on tri-colored sum-free sets in characteristic 2

Robert Kleinberg

May 27, 2016

## Abstract

A tri-colored sum-free set in an abelian group  $H$  is a collection of ordered triples in  $H^3$ ,  $\{(a_i, b_i, c_i)\}_{i=1}^m$ , such that the equation  $a_i + b_j + c_k = 0$  holds if and only if  $i = j = k$ . Using a variant of the lemma introduced by Croot, Lev, and Pach in their breakthrough work on arithmetic-progression-free sets, we prove that the size of any tri-colored sum-free set in  $\mathbb{F}_2^n$  is bounded above by  $6 \binom{n}{\lfloor n/3 \rfloor}$ . This upper bound is tight, up to a factor subexponential in  $n$ : there exist tri-colored sum-free sets in  $\mathbb{F}_2^n$  of size greater than  $\binom{n}{\lfloor n/3 \rfloor} \cdot 2^{-\sqrt{16n/3}}$  for all sufficiently large  $n$ .

## 1 Introduction

In a breakthrough paper, Croot et al. [2016] applied the polynomial method to prove that for sufficiently large  $n$ , every set of more than  $(3.62)^n$  elements of  $(\mathbb{Z}/4\mathbb{Z})^n$  contains a three-term arithmetic progression. This was the first such bound of the form  $c^n$  for a constant  $c < 4$ . Soon afterward, Ellenberg [2016] and, independently, Gijswijt [2016] extended the argument to prove an upper bound of the form  $c(p)^n$  on the size of any subset of  $\mathbb{F}_p^n$  that is free of three-term arithmetic progressions, where  $p$  is any odd prime and  $c(p)$  is a constant strictly less than  $p$ . Gijswijt provides the explicit bound  $c(p) < e^{-1/18}p$ .

In all of the aforementioned results, the upper bound obtained using the new methods is of the form  $C^n$  and the best known lower bound on the size of arithmetic-progression-free sets is of the form  $c^n$  for some  $c < C$ . Thus, in all known cases, there is still an exponential gap between the best known upper and lower bounds for such sets. In this note, we present a variant of the problem of finding large sets that contain no three-term arithmetic progressions, and we prove upper and lower bounds that differ by a sub-exponential factor — i.e., an upper bound of the form  $c^{n+o(n)}$  and a lower bound of the form  $c^{n-o(n)}$ , with the same constant  $c$  appearing as the base of the exponent in both bounds — when the problem is restricted to the group  $\mathbb{F}_2^n$ . The upper bound proof is an application of the lemma of Croot et al. [2016], while the lower bound follows from a construction due to Fu and Kleinberg [2014], which in turn utilizes a construction from Coppersmith and Winograd [1990].

Since vector spaces over a field of characteristic 2 have no three-term arithmetic progressions, it is not immediately clear how to generalize these questions to the case of characteristic 2. The following generalization was proposed and analyzed by Blasiak et al. [2016].

**Definition 1.** A tri-colored sum-free set in an abelian group  $H$  is a collection  $\{(a_i, b_i, c_i)\}_{i=1}^m$  of ordered triples in  $H^3$  such that the equation  $a_i + b_j + c_k = 0$  holds if and only if  $i = j = k$ .

Note that if  $H$  is an abelian group of odd order and  $A = \{a_1, \dots, a_m\} \subseteq H$ , then  $A$  contains no three-term arithmetic progressions if and only if the set  $\{(a_i, a_i, -2a_i)\}$  is a tri-colored sum-free set. Thus, upper bounds on the size of tri-colored sum-free sets immediately yield upper bounds on sets with no three-term arithmetic progressions, but the definition of tri-colored sum-free sets is meaningful even when  $H = \mathbb{F}_2^n$ .

## 2 Upper Bound

To prove an upper bound on the size of tri-colored sum-free sets in  $\mathbb{F}_p^n$ , we will introduce another closely related definition.

**Definition 2.** A *perfectly matched sequence* in an abelian group  $H$  is a sequence of ordered pairs  $\{(a_i, b_i)\}_{i=1}^m$  in  $H^2$  such that the equation  $a_i + b_i = a_j + b_k$  has no solutions with  $j \neq k$ . The set  $T = \{a_i + b_i \mid i = 1, \dots, m\}$  is called the *target set* of the perfectly matched sequence.

Note that if  $\{(a_i, b_i, c_i)\}$  is a tri-colored sum-free sequence of size  $m$ , then  $\{(a_i, b_i)\}$  is a perfectly matched sequence whose target set  $T = \{-c_i\}$  has  $m$  elements. The following theorem therefore yields an upper bound on the size of tri-colored sum-free sequences.

**Theorem 1.** Let  $L_n$  denote the linear subspace of  $\mathbb{F}_p[x_1, \dots, x_n]$  spanned by monomials of the form  $\prod_{i=1}^n x_i^{\alpha_i}$ , where  $0 \leq \alpha_i < p$  for all  $i$ , and let  $L_{n,d}$  denote the subspace of  $L_n$  spanned by monomials of degree at most  $d$ . The target set of any perfectly matched sequence in  $\mathbb{F}_p^n$  has at most  $3 \dim L_{n,d}$  elements, where  $d = \lfloor \frac{1}{3}(p-1)n \rfloor$ .

*Proof.* The proof is a recapitulation of the proof of Gijswijt [2016], Theorem 2, which corresponds to the special case when  $a_i = b_i$  for all  $i$ . We reiterate the proof here to facilitate the task of verifying that Gijswijt's proof extends to the general case.

Let  $V$  denote the vector space of polynomials  $f \in L_{n,(p-1)n-d-1}$  such that  $f(x) = 0$  for all  $x \notin T$ . The dimension of  $L = L_{n,(p-1)n-d-1}$  is equal to  $p^n - \dim L_{n,d}$ , and  $V$  is obtained from  $L$  by imposing an additional  $p^n - |T|$  linear constraints, one for each  $x \notin T$ . Hence  $\dim V \geq |T| - \dim L_{n,d}$ .

The evaluation map  $V \rightarrow \mathbb{F}_p^T$  is injective — see [Gijswijt, 2016], Proposition 1 — hence there is a set  $S \subseteq T$  of cardinality  $|S| = \dim V$  such that the evaluation map  $V \rightarrow \mathbb{F}_p^S$  is bijective. Choose a polynomial  $f \in V$  such that  $f(x) = 1$  for all  $x \in S$ , and consider the  $(2n)$ -variate polynomial

$$g(x_1, \dots, x_n, y_1, \dots, y_n) = f(x + y).$$

For a pair of multi-indices  $\alpha, \beta \in \{0, \dots, p-1\}^n$ , let  $C_{\alpha, \beta}$  denote the coefficient of the monomial  $x^\alpha y^\beta$  in  $g$ . Our choice of  $d = \lfloor \frac{1}{3}(p-1)n \rfloor$  ensures that  $(p-1)n - d - 1 \leq 2d + 1$ , so  $f \in L_{n, 2d+1}$  and, consequently, for every monomial  $x^\alpha y^\beta$  occurring in  $g$  either  $x^\alpha$  or  $y^\beta$  has degree at most  $d$ . Hence, the non-zero entries of  $C$  belong to the union of a set of rows and a set of columns each indexed by a set of  $\dim L_{n,d}$  monomials. Accordingly,  $\text{rank } C \leq 2 \dim L_{n,d}$ . On the other hand, the rank of  $C$  is bounded below by the rank of the matrix  $M_{i,j} = f(a_i + b_j)$ ; see Gijswijt [2016], Lemma 2. By construction,  $M_{i,j} = 0$  when  $i \neq j$  and  $M_{i,i} = 1$  when  $a_i + b_i \in S$ . Hence,

$$|S| \leq \text{rank } M \leq \text{rank } C \leq 2 \dim L_{n,d}.$$

Recalling that  $|S| = \dim V \geq |T| - \dim L_{n,d}$ , we obtain the inequality  $|T| \leq 3 \dim L_{n,d}$  as claimed.  $\square$

When  $p = 2$ , we have  $\dim L_{n,d} = \sum_{k=0}^{\lfloor n/3 \rfloor} \binom{n}{k} < 2 \binom{n}{\lfloor n/3 \rfloor}$ . This bound, in conjunction with Theorem 1, implies the upper bound on tri-colored sum-free sets in  $\mathbb{F}_2^n$  stated in the abstract.

### 3 Lower Bound

Our lower bound on the size of tri-colored sum-free sets  $\mathbb{F}_2^n$  recapitulates a construction due to Fu and Kleinberg [2014] which, in turn, is based on a method originating in the work of Coppersmith and Winograd [1990] on fast matrix multiplication. We shall make use of the fact that the cyclic group  $\mathbb{Z}/M\mathbb{Z}$ , for large  $M$ , has subsets of size  $M^{1-o(1)}$  which contain no three-term arithmetic progressions. The best known lower bound on the size of such subsets is the following theorem of Elkin [2011]; see also Green and Wolf [2010]. (In the theorem statement, the expression  $\log(\cdot)$  denotes the base-2 logarithm.)

**Theorem 2** (Elkin, 2011). *For all sufficiently large  $M$ , the group  $\mathbb{Z}/M\mathbb{Z}$  has a subset of size greater than  $\log^{1/4}(M) \cdot 2^{-\sqrt{8 \log M}} \cdot M$  which contains no three distinct elements in arithmetic progression.*

Assume for simplicity that  $n$  is divisible by 3. (When  $n$  is indivisible by 3, we may take a large tri-colored sum-free set in  $\mathbb{F}_2^{n'}$  for  $n' = 3\lfloor n/3 \rfloor$  and “pad” each vector with 0’s to obtain an equally large tri-colored sum-free set in  $\mathbb{F}_2^n$ .) Let  $M$  be an odd integer greater than  $4^{\binom{2n/3}{n/3}}$ . Our tri-colored sum-free set will be constructed as a subset of the set  $X$  of all triples  $(a, b, c) \in (\{0, 1\}^n)^3$  such that the vectors  $a, b, c$  have Hamming weights  $\frac{n}{3}, \frac{n}{3}, \frac{2n}{3}$ , respectively, and  $c = a + b$ . Note that for any  $(a, b, c) \in X$ , the equation  $c = a + b$  holds regardless of whether the left and right sides are interpreted as vectors over  $\mathbb{F}_2$  or over  $\mathbb{Z}$ .

Letting  $W = (\mathbb{Z}/M\mathbb{Z})^{n+1}$  we now define three functions  $h_0, h_1, h_2 : \{0, 1\}^n \times W \rightarrow \mathbb{Z}/M\mathbb{Z}$  as follows.

$$h_0(a, w) = \sum_{s=1}^n a_s w_s, \quad h_1(b, w) = \frac{1}{2} \left( w_0 + \sum_{s=1}^n b_s w_s \right), \quad h_2(c, w) = w_0 + \sum_{s=1}^n c_s w_s.$$

The function  $h_1$  is well-defined because  $\mathbb{Z}/M\mathbb{Z}$  is a cyclic group of odd order. By construction, whenever  $a, b, c$  are three vectors satisfying  $a + b = c$  (over  $\mathbb{Z}$ ), the values  $h_0(a, w), h_1(b, w), h_2(c, w)$  are either identical or they form an arithmetic progression in  $\mathbb{Z}/M\mathbb{Z}$ . Now, fix a set  $B \subset \mathbb{Z}/M\mathbb{Z}$  that contains no three distinct elements in arithmetic progression. For any  $w \in W$  define sets  $Y(w), Y_0(w), Y_1(w), Y_2(w), Y_3(w), Z(w)$  as follows.

$$\begin{aligned} Y(w) &= \{(a, b, c) \in X \mid h_0(a, w), h_1(b, w), h_2(c, w) \in B\} \\ Y_0(w) &= \{(a, b, c) \in Y(w) \mid \exists (b', c') \neq (b, c) \text{ s.t. } (a, b', c') \in Y(w)\} \\ Y_1(w) &= \{(a, b, c) \in Y(w) \mid \exists (a', c') \neq (a, c) \text{ s.t. } (a', b, c') \in Y(w)\} \\ Y_2(w) &= \{(a, b, c) \in Y(w) \mid \exists (a', b') \neq (a, b) \text{ s.t. } (a', b', c) \in Y(w)\} \\ Z(w) &= Y(w) \setminus (Y_0(w) \cup Y_1(w) \cup Y_2(w)). \end{aligned}$$

We first claim that  $Z(w)$  is a tri-colored sum-free set. The equation  $a + b + c = 0$  holds in  $\mathbb{F}_2^n$  for every  $(a, b, c) \in Z(w)$ , by construction, so we need only verify conversely that for any three (not necessarily distinct) elements  $(a, b, c), (a', b', c'), (a'', b'', c'')$  of  $Z(w)$ , if the equation  $a + b' + c'' = 0$  holds in  $\mathbb{F}_2^n$  then all three of the given elements of  $Z(w)$  are equal to one another. Indeed, our hypotheses about  $(a, b, c), (a', b', c'), (a'', b'', c'')$  imply all of the following conclusions about  $(a, b', c'')$ :

1.  $a$  and  $b'$  have Hamming weight  $n/3$ , while  $c''$  has Hamming weight  $2n/3$ ;
2.  $c'' = a + b'$ ;
3.  $h_0(a, w), h_1(b', w), h_2(c'', w) \in B$ .

In other words,  $(a, b', c'')$  belongs to  $Y(w)$ . The fact that  $(a, b, c) \notin Y_0(w)$  now implies that  $(a, b, c) = (a, b', c'')$ . Similarly, the facts that  $(a', b', c') \notin Y_1(w)$  and  $(a'', b'', c'') \notin Y_2(w)$  imply that  $(a', b', c') = (a'', b'', c'') = (a, b', c'')$ . Thus, the three given elements of  $Z(w)$  are all equal to one another, as required by the definition of a tri-colored sum-free set.

Let us now prove a lower bound on the expected cardinality of  $Z(w)$  when  $w$  is chosen uniformly at random from  $(\mathbb{Z}/M\mathbb{Z})^{n+1}$ . For a given element  $(a, b, c) \in X$ , the values  $h_0(a, w), h_1(b, w), h_2(c, w)$  must either be equal to one another or they must form an arithmetic progression. The set  $B$  contains no three elements in arithmetic progression, so the event that  $h_0(a, w), h_1(b, w), h_2(c, w) \in B$  coincides with the event that there exists  $\beta \in B$  such that  $h_0(a, w) = h_1(b, w) = h_2(c, w) = \beta$ ; furthermore, if any two of  $h_0(a, w), h_1(b, w), h_2(c, w)$  are equal to  $\beta$ , then so is the third. For  $w$  uniformly distributed in  $(\mathbb{Z}/M\mathbb{Z})^{n+1}$ , the values  $h_0(a, w)$  and  $h_2(c, w)$  are independent and uniformly distributed in  $\mathbb{Z}/M\mathbb{Z}$ , so the probability of the event  $h_0(a, w) = h_2(c, w) = \beta$  is  $M^{-2}$ . Summing over all  $\beta \in B$  and all  $(a, b, c) \in X$ , we find that the expected cardinality of  $Y(w)$  is

$$\mathbb{E}|Y(w)| = |X| \cdot |B| \cdot M^{-2} = \binom{n}{n/3} \cdot \binom{2n/3}{n/3} \cdot |B| \cdot M^{-2}. \quad (1)$$

Similar reasoning allows us to derive an upper bound the expected cardinality of  $Y_0(w)$ . If  $(a, b, c)$  belongs to  $Y_0(w)$  it means that there is some other element  $(a, b', c') \in X$  and some  $\beta \in B$  such that

$$h_0(a, w) = h_1(b, w) = h_2(c, w) = h_1(b', w) = h_2(c', w) = \beta. \quad (2)$$

For  $w$  uniformly distributed in  $(\mathbb{Z}/M\mathbb{Z})^{n+1}$ , the values  $h_0(a, w), h_2(c, w)$ , and  $h_2(c', w)$  are independent and uniformly distributed in  $\mathbb{Z}/M\mathbb{Z}$ ; this is most easily verified by checking that  $h_0(a, w), h_2(c, w)$ , and  $h_2(c, w) - h_2(c', w)$  are independent and uniformly distributed. Furthermore, if  $h_0(a, w) = h_2(c, w) = h_2(c', w) = \beta$  then  $h_1(b, w) = h_1(b', w) = \beta$ , so the probability of the event indicated in (??) is  $|M|^{-3}$ . Summing over all pairs of distinct elements  $(a, b, c), (a, b', c') \in X$  that share the same first coordinate, and all  $\beta \in B$ , we find that the expected cardinality of  $Y_0(w)$  is at most

$$\mathbb{E}|Y_0(w)| \leq |X| \cdot \left( \binom{2n/3}{n/3} - 1 \right) \cdot |B| \cdot M^{-3} = \mathbb{E}|Y(w)| \cdot \frac{1}{M} \left( \binom{2n/3}{n/3} - 1 \right) < \frac{1}{4} \mathbb{E}|Y(w)| \quad (3)$$

where the last inequality is justified by our choice of  $M > 4 \binom{2n/3}{n/3}$ . Analogous reasoning yields the bounds  $\mathbb{E}|Y_1(w)|, \mathbb{E}|Y_2(w)| < \frac{1}{4} \mathbb{E}|Y(w)|$ , and hence

$$\mathbb{E}|Z(w)| \geq \mathbb{E}|Y(w)| - \mathbb{E}|Y_0(w)| - \mathbb{E}|Y_1(w)| - \mathbb{E}|Y_2(w)| > \frac{1}{4} \mathbb{E}|Y(w)| = \frac{1}{4} \cdot \frac{1}{M} \binom{2n/3}{n/3} \cdot \frac{|B|}{M} \cdot \binom{n}{n/3}.$$

If  $n$  is sufficiently large, then for  $M = 4 \binom{2n/3}{n/3} + 1$  and  $B > \log^{1/4}(M) \cdot 2^{-\sqrt{8 \log M}} \cdot M$  we have

$$\frac{1}{4} \cdot \frac{1}{M} \binom{2n/3}{n/3} \cdot \frac{|B|}{M} > 2^{-\sqrt{16n/3}},$$

hence

$$\mathbb{E}|Z(w)| > \binom{n}{n/3} \cdot 2^{-\sqrt{16n/3}} > \binom{n}{n/3}^{1-o(1)}$$

as claimed.

## References

- Blasiak, J., Church, T., Cohn, H., Grochow, J. A., and Umans, C. (2016). On cap sets and the group-theoretic approach to matrix multiplication. arXiv:1605.06702 [math.CO].
- Coppersmith, D. and Winograd, S. (1990). Matrix multiplication via arithmetic progressions. *J. Symbolic Computation*, 9(3):250–280.
- Croot, E., Lev, V., and Pach, P. (2016). Progression-free sets in  $\mathbb{Z}_4^n$  are exponentially small. arXiv:1605.01506 [math.NT].
- Elkin, M. (2011). An improved construction of progression-free sets. *Israeli J. Math.*, 184:93–128.
- Ellenberg, J. S. (2016). On large subsets of  $\mathbb{F}_3^n$  with no three-term arithmetic progression. Manuscript.
- Fu, H. and Kleinberg, R. (2014). Improved lower bounds for testing triangle-freeness in boolean functions via fast matrix multiplication. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, 17th International Workshop, APPROX 2014, and 18th International Workshop, RANDOM 2014*. arXiv:1308.1643 [cs.CC].
- Gijswijt, D. (2016). Asymptotic upper bounds on progression-free sets in  $\mathbb{Z}_p^n$ . arXiv:1605.05492 [math.CO].
- Green, B. and Wolf, J. (2010). A note on Elkin’s improvement of Behrend’s construction. In *Additive number theory*, pages 141–144. Springer.